AO 106A (08/18) Application for a Warrant by Telephone or Other Reliable Electronic Means

UNITED STATES DISTRICT COURT

for the

Western District of Virginia ☐

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)
Information associated with Google account ID 143infinity.n.beyond@gmail.com that is stored at premises controlled by Google

Case No. 1:21mj27

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attachment A

located in the Northern District of California, there is now concealed *(identify the person or describe the property to be seized):*

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more):*

- ☑ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
21 USC 846	Conspiracy to Distribute and Possess with Intent to Distribute Methamphetamine

The application is based on these facts:

See attached Affidavit

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days *(give exact ending date if more than 30 days: _____)* is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Senior Special Agent Ryan Temm
Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone *(specify reliable electronic means).*

Date: 2/2/21

Judge's signature

City and state: Abingdon, VA

Pamela Meade Sargent USMJ
Printed name and title

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with **143infinity.n.beyond@gmail.com** that is stored at premises owned, maintained, controlled, or operated by Google, a company headquartered at 1600 Amphitheatre Parkway, Mountain View, CA 94043.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Google (the "Provider")

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, regardless of whether such information is located within or outside of the United States, and including any emails, records, files, logs, or information that has been deleted but is still available to the Provider, or has been preserved pursuant to the request made under 18 U.S.C. § 2703(f) on January 14, 2021, the Provider is required to disclose the following information to the government for the account or identifier listed in Attachment A:

A. The contents of all emails associated with the account from January 1, 2020, to Present Day, including stored or preserved copies of emails sent to and from the account, draft emails, the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each email;

B. All records or other information regarding the identification of the account or linked to the account, to include full name, physical address, telephone numbers and other identifiers, any and all data stored as part of the individual's use of the following Google services: 3D Warehouse, AdManager, AdPlanner, AdSense, AdWords, Alerts, Analytics, Apps, Base, Blogger, Bookmarks, Buzz, Calendar, Checkout, Contacts, Dashboard, Docs, Friend Connect, Groups, Health, Merchant Center, Notebook, Orkut, Picasa, Profiles, Reader, Talk, Tasks, Voice, and Wave; records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, device identifiers associated with any device that has logged into this account or device that has been linked to this account, alternative email addresses or phone numbers provided during registration, account recovery methods including any form of contact information provided, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

C. All Backup files, stored in Google Drive or elsewhere, including associated data such as application data call history, device settings, contacts, calendar information, short message system files consisting of data, time, sender, receiver, and message content, photos and videos;

D. Android Information-Device make, model, and International Mobile Equipment Identifier (IMEI) or Mobile Equipment Identifier (MEID) of all associated devices linked to **143infinity.n.beyond@gmail.com**;

E. Contacts -- All contacts stored by Google including name, all contact phone numbers, emails, social network links, and images;

F. All Chrome data including autofill, bookmarks, browser history, extensions, dictionary, search engine, and sync settings;

G. Gmail -- All email messages, including by way of example and not limitation, such as inbox messages whether read or unread, sent mail, saved drafts, chat histories, and emails in the trash folder. Such messages will including all information such as the date, time, internet protocol (IP) address routing information, sender, receiver, subject line, any other parties sent the same electronic mail through the "cc" (carbon copy) or the "bcc" (blind carbon copy), the message content or body, and all attached files;

H. Google Photos – All images, graphic files, video files, and other media files stored in the Google Photos service;

I. Google Maps -- All Google Maps data including commute routes, commute settings, and labeled places;

J. Google Location History / Google Timeline data for any devices associated with **143infinity.n.beyond@gmail.com** to include, but not limited to, all location data whether derived from Global Positioning System (GPS), cell site / cell tower triangulation / multi-alteration, precision measurement information such as timing advance, or per call measurement data, Wi-Fi location, Bluetooth, or device sensors, including accelerometer, barometer, gravity, magnetic field, orientation, or proximity. Such data shall include the GPS coordinates and the dates and times of all location recordings from the period of January 1, 2020, to December 31, 2020;

K. Play Store -- All applications downloaded, installed, and / or purchased by **143infinity.n.beyond@gmail.com**;

L. Web and Application history – All search history and queries, including by way of example and not limitation, World Wide Web (web) browsing, images, news, shopping, ads, videos, maps, travel, and finance, whether performed in private browsing, incognito, anonymous or secret mode, all device activity including application use, social media use, device phone

functions such as calling and/or text messaging activity, email activity including read, sent, and received emails, and the dates and times of searches made and applications used;

M. Voice – All call detail records, connection records, short message system (SMS) or multimedia message system (MMS) messages, and voicemail messages sent by or from the Google Voice account associated with **143infinity.n.beyond@gmail.com**;

N. Docs (Documents) – All Google documents including by way of example and not limitation, Docs (a web-based word processing application) and Sheets (a web-based spreadsheet program). Documents will include all files whether created, shared, or downloaded;

O. The types of service utilized;

P. All records or other information stored by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files;

Q. All location information pertaining to the account or linked to the account from the time period of January 1, 2020 to December 31, 2020;

R. All records pertaining to communications between the Provider and any person regarding the account, including contacts with support services and records of actions taken.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, contraband, evidence, and/or instrumentalities of the statute listed on the warrant, for the account or identifier listed in Attachment A, including information pertaining to the following matters:

A. All records or information, including the contents of any and all wire and electronic communications, attachments, header information, or other stored files, that will assist investigators in ascertaining the nature and scope of the crime under investigation; the true identity and/or location of the suspect and any co-conspirators; and any disposition of the proceeds of the crime under investigation; and

B. Records related to who created, used, or communicated with the account or identifier.

AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR A SEARCH WARRANT

I, Ryan C. Temm, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information associated with 143infinity.n.beyond@gmail.com that is stored at premises owned, maintained, controlled, or operated by Google Inc. (hereafter "Google"), an email and cloud storage provider headquartered at 1600 Amphitheatre Parkway, Mountain View, CA 94043. The information to be searched is described in the following paragraphs and Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Google to disclose to the government records and other information (including the content of communications) in its possession, pertaining to the subscriber or customer associated with the user 143infinity.n.beyond@gmail.com.
2. I am an investigative law enforcement officer of the United States within the meaning of Section 2510(7) of Title 18 United States Code, and am empowered by law to conduct investigations and to make arrests for the offenses enumerated in Section 2516 of Title 18 United States Code.
3. I am a Senior Special Agent (SSA) with the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF). I have been employed by ATF for over twelve (12) years. I received my training with the Federal Law Enforcement Training Center (FLETC), and the ATF at the National Academy in Brunswick, Georgia. At the ATF National Academy, we trained in various investigative techniques, including preparing a proper search warrant. Since becoming a Special Agent with ATF, I have participated in numerous search and arrest warrants. I have a Bachelor of Arts Degree in Criminal Justice from George Washington University and a Master of Public Administration from the University of North Carolina at Charlotte. I also successfully completed a basic law enforcement academy with the Charlotte-Mecklenburg Police Department and served nearly eight years as a police officer.
4. Based on my training and experience, I am familiar with methods used by drug traffickers to smuggle and safeguard narcotics, distribute narcotics, and collect and launder proceeds. I am aware of the sophisticated tactics drug traffickers routinely use to attempt to thwart detection by law enforcement, which include utilizing numerous different cellular

telephones, counter surveillance, elaborately planned distribution schemes, false or fictitious identities, and coded communications and conversations.

5. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

6. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that 143infinity.n.beyond@gmail.com, described in Attachment A, contains electronically stored information, as described in Attachment B, consisting of evidence, instrumentalities, contraband, and/or fruits of violating 21 U.S.C. § 846, Conspiracy to Possess with Intent to Distribute Methamphetamine. There is also probable cause to search the information described in Attachment A for evidence of this crime and contraband or fruits of this crime, as described in Attachment B.

PROBABLE CAUSE

7. On December 15, 2020, ATF Special Agent (SA) Peter Gonzalves interviewed Kristopher Tremblay at the United States District Courthouse in Abingdon, Virginia. Tremblay is a cooperating defendant in the Western District of Virginia, and he agreed to an interview with the consent of his counsel. Tremblay stated he believes Hunter Stone PHILLIPS ("PHILLIPS") has access to a mobile device while incarcerated in Georgia and is presently using Facebook Messenger to coordinate trafficking of controlled substances, including methamphetamine, between Georgia and persons located in Lee, Wise and Scott Counties, Virginia, within the Western District of Virginia. Tremblay also has made statements to law enforcement indicating he travelled from Virginia to Georgia with Tiffany VANOVER, another charged defendant in the Western District of Virginia, to procure methamphetamine through PHILLIPS.

8. On January 8, 2021, Southwest Drug Task Force Agent Kenneth Hill and I interviewed CS-1 at the Southwest Virginia Regional Jail at Duffield. The information contained in Paragraphs 9 through 14 of this Affidavit represent a summary of relevant information provided by CS-1 during the interview.

9. CS-1 has been dealing with Hunter Stone PHILLIPS to buy methamphetamine. CS-1's purchases of methamphetamine through PHILLIPS began sometime after May 26, 2020, when Tiffany VANOVER called him/her and told him/her to go get VANOVER's drug runner, "Rod", who I know to be Gregory CLINE, out of jail. CS-1 went and got Rod out

of jail and they went to Rod's brother's trailer at a trailer park in Silva, North Carolina, where Rod was supposed to have methamphetamine waiting in a car. CS-1 was supposed to ride back to Virginia and take the methamphetamine to VANOVER. The methamphetamine for VANOVER had already been paid for.

10. When "Rod" got to the trailer park in Silva, North Carolina, he disappeared. CS-1 called PHILLIPS and asked him what to do. PHILLIPS told him/her to knock on all the doors and find Rod. CS-1 finally found Rod "nodded out" in a trailer. Eventually, VANOVER obtained approximately 7 ounces of methamphetamine. CS-1 witnessed VANOVER weigh out the methamphetamine at his/her (CS-1) trailer.
11. During the drive to pick up Rod, VANOVER gave CS-1 PHILLIPS's phone number. PHILLIPS was supposed to pay the bond necessary to get Rod out of jail.
12. After VANOVER was arrested on September 26, 2020, sometime in October 2020, CS-1 called PHILLIPS at the phone number provided by VANOVER and PHILLIPS told CS-1 he would get him/her five ounces of methamphetamine for $2,200. CS-1 sent money to PHILLIPS via Western Union to purchase the methamphetamine. CS-1 said he/she saved everything required for the methamphetamine purchase, including the addresses and directions of the places to which he/she drove to pick up the methamphetamine, on her Google Drive, which uses the username 143infinity.n.beyond@gmail.com.
13. For the last three and a half months, since VANOVER's arrest, CS-1 has been travelling between the Western District of Virginia, North Carolina, and Georgia to purchase methamphetamine through PHILLIPS. In October 2020, he/she made four trips to pick up methamphetamine through PHILLIPS. CS-1 called PHILLIPS and PHILLIPS told him/her where to go to obtain the methamphetamine. Most of the first trips to obtain the methamphetamine were from Virginia to North Carolina.
14. In December 2020, CS-1, Jon ROLLINS, who is another charged defendant in the Western District of Virginia, and Cody Phipps went from Virginia to Georgia to purchase methamphetamine on an almost daily basis, obtaining five to eighteen ounces of methamphetamine at a time. They dropped the methamphetamine they purchased off at the home of Jessica ROBEY, another charged defendant in the Western District of Virginia, in Big Stone Gap, Virginia.
15. On January 14, 2021, a preservation request was sent to Google to preserve data associated with the 143infinity.n.beyond@gmail.com account.

BACKGROUND CONCERNING GOOGLE

16. Based upon my training and experience, and information acquired from other law enforcement officials with technical expertise, I have learned the following information. Google provides a variety of online services to the public, including electronic mail ("email"). Google allows subscribers to obtain email accounts at the domain name gmail.com, like the email account listed in Attachment A. Subscribers obtain an account by registering with Google. During the registration process, Google asks subscribers to provide basic personal information. Google maintains information about the mobile devices associated with the subscribers' Google accounts. This includes the make, model, and unique serial numbers of all linked devices. Google also maintains information about its subscribers, including primary email addresses, secondary email addresses for account password recovery, applications, websites, and services that are allowed to access the subscribers' Google accounts or use the subscribers' Google accounts as a password login, and account login activity such as the geographic area in which a subscriber logged into their account, what type of internet browser and/or device the subscriber was using, and the internet protocol (IP) address from which they logged in. The IP address is roughly analogous to a telephone number assigned to a computer by an internet service provider. The IP address can be resolved back to a physical address, such as a residence or business with Wi-Fi access or residential cable internet. I believe this information will assist in the investigation by identifying previously unknown email accounts and devices utilized by the suspect, as well as location history information tending to show the movements of the suspect and his/her mobile device(s).

17. Google subscribers can enroll Android devices with an associated Google account into a device backup service. This backup service duplicates some of the information stored on the device in the event the user loses their device or it becomes otherwise inoperable. Device backup data is limited to data from applications stored on the device, all history including dialed, received, and missed calls, and device settings. The backup files are named with the device's manufacturer and model number in the user's Google Drive service.

18. A Google subscriber can also store with the provider other files in addition to emails, such as address books, favorite locations, contact or buddy lists, calendar data, pictures, and videos, on servers maintained and/or owned by Google. In my training and experience, evidence of who was using an email account may be found in address books, contact or buddy lists, emails in the account, and attachments to emails, including pictures and files,

as well as in the location history. I believe this information could show the suspect's location at the time the above-mentioned drug transactions were committed.

19. Google Maps is a web service and application that allows users to search for places and routes to navigate using public transportation, vehicle, bicycle, or foot. Users can label or designate specific places in Google such as home or work. Google maps also records commute routes and commute settings based on recorded patterns such as date and time, origin and destination, and route traveled. I believe this information would allow law enforcement to show patterns of travel, which may corroborate or disprove other evidence in this case.

20. Chrome is an internet browser developed and distributed by Google. The Chrome browser is tightly integrated with other Google products and is the default browser installed on the Android operating system. The Chrome browser collects and stores information which is transmitted to Google and retained by the company. This information includes autofill and auto-populate data from prior searches, bookmarked webpages, browser history showing searched-for words, extensions and add-ons that are developed by Google and third-parties to bring custom features to the browser, search engines used, and sync settings so the user can have the previously listed features across multiple devices. I believe this information would show the suspect's internet activity during the drug trafficking activity described above.

21. In my training and experience, email providers generally ask their subscribers to provide certain personal identifying information when registering for an email account. Such information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative email addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number). In my training and experience, such information may constitute evidence of crimes under investigation because the information can be used to identify the account's user or users. Based on my training and my experience, I know that, even if subscribers insert false information to conceal their identity, this information often provides clues to their identity, location, or illicit activities.

22. In my training and experience, email providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (*i.e.*, session) times and durations, the types of services utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the

account (such as logging into the account via the provider's website), and other log files that reflect usage of the account.

23. In my training and experience, in some cases, email account users will communicate directly with an email service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Email providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user as a result of the communications. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

24. As explained herein, information stored in connection with an email account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling law enforcement to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, the information stored in connection with an email account can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, email communications, contacts lists, and images sent (and the data associated with the foregoing, such as date and time) may indicate who used or controlled the account at a relevant time. Further, information maintained by the email provider can show how and when the account was accessed or used. For example, as described above, email providers typically log the Internet Protocol (IP) addresses from which users access the email account, along with the time and date of that access. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the email account access and use relating to the crime under investigation. This geographic and timeline information may tend to either inculpate or exculpate the account owner. Additionally, information stored at the user's account may further indicate the geographic location of the account user at a particular time (*e.g.*, location information integrated into an image or video sent via email). Last, stored electronic data may provide relevant insight into the email account owner's state of mind as it relates to the offense under investigation. For example, information in the email account may indicate the owner's motive and intent to commit a crime (*e.g.*, communications relating to the crime), or consciousness of guilt (*e.g.*, deleting communications in an effort to conceal them from law enforcement).

25. Searching for the evidence described in this warrant application may require a range of data analysis techniques. In some cases, law enforcement officers and computer analysts may be able to conduct carefully targeted searches to locate evidence without needing to carry out a time-consuming manual search through unrelated materials that may be commingled with criminal evidence. In other cases, however, such techniques may not yield the evidence described in the warrant. Numerous types of user information and metadata stored on a cellphone are not susceptible to "word search" or similar forensic techniques, including but not limited to images, audio and video recordings, and proximate GPS locations. In addition, the complex interrelatedness of cell-phone data may undermine the efficacy of narrow search techniques based on the type, location, or date of information. Indeed, the vast array of applications now available on cellular telephones makes it extremely hard to determine the exact form and organization of user information and metadata prior to conducting a search. Finally, criminals can mislabel, misspell, or hide information; encode communications to avoid using key words; attempt to delete information to evade detection; or take other steps designed to frustrate law enforcement searches for information.
26. Accordingly, law enforcement officials or other analysts with appropriate expertise may need to conduct more extensive searches not obviously related to the evidence described in this warrant application or perusing all stored information briefly to determine whether it falls within the scope of the warrant. In light of these difficulties, ATF and its partners intend to use whatever data analysis techniques appear necessary to locate and retrieve the evidence described in this warrant application.
27. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant. The government will execute this warrant by serving the warrant on Google. Because the warrant will be served on Google, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

28. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require Google to disclose to the government copies of the records and other information (including the content of communications) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B,

government-authorized persons will review that information to locate the items described in Section II of Attachment B.

CONCLUSION

29. Based on the forgoing, I request that the Court issue the proposed search warrant.
30. This Court, the United States District Court for the Western District of Virginia, has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711 and 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A).
31. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

Respectfully submitted,

Senior Special Agent Ryan C. Temm
Bureau of Alcohol, Tobacco, Firearms, and Explosives
United States Department of Justice

Subscribed and sworn to before me on Telephonically February 2, 2021

Pamela Meade Sargent

United States Magistrate Judge Pamela Meade Sargent

Reviewed by: Lena Busscher, AUSA